UNITED STATES PATENT AND TRADEMARK OFFICE

**UNITED STATES DEPARTMENT OF COMMERCE**
**United States Patent and Trademark Office**
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/015,886 | 12/17/2001 | Steve Vlcan | CIT10314 | 7290 |

75127 7590 09/16/2009

KING & SPALDING LLP (CITI CUSTOMER NUMBER)
ATTN: GEORGE T. MARCOU
1700 PENNSYLVANIA AVENUE, NW
SUITE 200
WASHINGTON, DC 20006

| EXAMINER | |
|---|---|
| MOORTHY, ARAVIND K | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2431 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 09/16/2009 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

# BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/015,886
Filing Date: December 17, 2001
Appellant(s): VLCAN ET AL.

Eric L. Sophir
Reg. No. 48,499
For Appellant

## EXAMINER'S ANSWER

This is in response to the appeal brief filed 12 June 2009 appealing from the Office action mailed 16 October 2008.

**(1) Real Party in Interest**

A statement identifying by name the real party in interest is contained in the brief.

**(2) Related Appeals and Interferences**

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

**(3) Status of Claims**

The statement of the status of claims contained in the brief is incorrect. A correct statement of the status of the claims is as follows:

Claims 5 and 13 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

**(4) Status of Amendments After Final**

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

**(5) Summary of Claimed Subject Matter**

The summary of claimed subject matter contained in the brief is correct.

**(6) Grounds of Rejection to be Reviewed on Appeal**

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

**(7) Claims Appendix**

The copy of the appealed claims contained in the Appendix to the brief is correct.

**(8) Evidence Relied Upon**

| | | |
|---|---|---|
| US 2002/0069363 A1 | Winburn | 06-2002 |
| 5,991,760 | Gauvin et al | 11-1999 |
| 5,909,429 | Satyanarayana et al | 06-1999 |

**(9) Grounds of Rejection**

The following ground(s) of rejection are applicable to the appealed claims:

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-3, 6, 7, 9-11, 14, 15, 17 and 18 are rejected under 35 U.S.C. 102(e) as being anticipated by Winburn US 2002/0069363 A1.

As to claims 1 and 10, Winburn discloses a method for maintaining the integrity of a file at a remote location via a communication medium, comprising the steps of:

performing an integrity check on the file by an integrity module [0030];

redirecting to an install module by a redirect module if the integrity check fails [0031],

wherein the step of redirecting to the install modules comprises the steps of:

modifying an address of the install module by the redirect module to include a parameter to indicate the remote location of the file [0027];

producing a request by an authentication module based on the modified address that indicates the remote location of the file [0028], and

communicating the request by the authentication module to the install module in a login page that instantiated the file at the remote location [0031]; and

reinstalling the file by the install module at the remote location via the communication medium, thereby maintaining the integrity of the file [0031].

As to claims 2 and 11, Winburn discloses that the step of performing the integrity check comprises the steps of:

using an algorithm on the file to produce a remote value [0027-0028];

communicating the remote value to the integrity module via the communication medium [0027-0028];

using the algorithm on a mirror file to produce a secure value, wherein the mirror file is a valid copy of the file [0027-0028]; and

communicating that the integrity check passed if the remote value and the secure value are equivalent [0027-0028].

As to claims 3 and 18, Winburn discloses that the algorithm is a hash algorithm [0027-0028].

As to claims 6 and 14, Winburn discloses that the communication medium is the Internet [0025].

As to claims 7 and 15, Winburn discloses that the communication medium is a local network [0025].

As to claims 9 and 17, Winburn discloses that the remote location is an authentication control component [0030].

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 8 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Winburn US 2002/0069363 A1 as applied to claims 1 and 10 above, and further in view of Satyanarayana et al U.S. Patent No. 5,909,429.

As to claims 8 and 16, Winburn does not teach that the communication medium is a wireless network.

Satyanarayana et al teaches a communication network that is a wireless network as well as its benefits [column 6 line 66 to column 7 line 9].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Winburn so that the communication medium was a wireless network.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Winburn by the teaching of Satyanarayana et al because wireless networks eliminate the need for connectors and wires at the, provides an opportunity for testing the operation of the nodes prior to completion of installation of the network (and prior to execution of the network initialization routine), and reduces the cost and time required for installation of the wireless network [column 9, lines 37-47].

**(10) Response to Argument**

A. The Appellant argues that Winburn does not disclose "modifying an address of the install module by the redirect module to include a parameter to indicate the remote location of the file," as recited in claim 1 and similarly recited in claim 10.

The examiner respectfully disagrees. Winburn discloses in FIGS. 2 and 5, the camouflaging process used in translation of the authorized protected file 31 to the saved authentic backup file 33, may use compression to change the data length, encryption by symmetric or asymmetric keys as would be known to those skilled in the art, and a change in file name and location, as shown by step (43) in FIG. 5, for storage as a camouflaged file in the storage devices 15, 17, 21 for example. By compression the relationship of size between the authentic backup file 33 and authorized protected data file 31 is changed. By encryption, the relationship of data content between the authentic backup file 33 and the authorized protected data file 31 is changed. By changing the authentic backup file 33 location(s) and name(s), the space relation between the authorized protected data file 31 and the authentic backup file 33 is changed. Changing or removing any relationships between the authentic backup file 33 and the authorized protected data file 31 serves to camouflage the authentic backup file 33 so any intrusion or unauthorized modification of the authorized protected data file 31, causing its compromise, will be preventing from extending to the discovery of the location or identity of the authentic backup file 33 [0026]. Winburn discloses that the stored indica is accessed and used to locate and translate the authentic backup file to reconstruct the authorized protected data backup file and restore the current protected data file to the authorized protected data file [0011].

B. The Appellant argues that Winburn does not disclose “reinstalling the file by the install module at the remote location via the communication medium,” as recited in claim 1 and similarly recited in claim 10.

The examiner respectfully disagrees. Winburn discloses that in order to protect the integrity of the authorized protected data files data contents, an authentic backup file 33 is constructed and its location and identity camouflaged to remove any direct relation between any of the attributes of the authorized protected data file and the corresponding authentic backup file. In its camouflaged state the authentic backup file 33 is maintained for later use in restoration of the authorized protected data file 31, in the event of a system intrusion, such as by an intruder in the system or by unauthorized access or modification of the authorized protected file. The method of creating an authentic backup file 33 for maintaining the authorized protected data file's 31 integrity is as shown in FIGS. 2 to 7, with FIGS. 2 to 4 showing in block form the system for initiating the protection of an authorized protected data file, monitoring the protected data file and restoring the protected data file and with FIGS. 5 to 7 showing the process for initiating the protection of an authorized protected data file, monitoring the protected data file and restoring the protected data file, with the numerals referring to the process steps in FIGS. 5 to 7, shown in parentheses [0026].

C. The Appellant argues that Winburn is not modifying an address of an install module to indicate the remote location of a file. The Appellant argues that instead, Winburn uses an indicia in an active or RAM memory in order to camouflage the location of a backup file. The Appellant argues that as a result, Winburn cannot modify an address of an install module, because an install module is not resident in active or RAM memory. The Appellant argues that recited in the specification, the install module is associated with a web/application server (106).

The examiner respectfully disagrees. Winburn discloses in FIGS. 2 and 5, the camouflaging process used in translation of the authorized protected file 31 to the saved authentic backup file 33, may use compression to change the data length, encryption by symmetric or asymmetric keys as would be known to those skilled in the art, and a change in file name and location, as shown by step (43) in FIG. 5, for storage as a camouflaged file in the storage devices 15, 17, 21 for example. By compression the relationship of size between the authentic backup file 33 and authorized protected data file 31 is changed. By encryption, the relationship of data content between the authentic backup file 33 and the authorized protected data file 31 is changed. By changing the authentic backup file 33 location(s) and name(s), the space relation between the authorized protected data file 31 and the authentic backup file 33 is changed. Changing or removing any relationships between the authentic backup file 33 and the authorized protected data file 31 serves to camouflage the authentic backup file 33 so any intrusion or unauthorized modification of the authorized protected data file 31, causing its compromise, will be preventing from extending to the discovery of the location or identity of the authentic backup file 33 [0027].

D. The Appellant argues that Winburn is not checking the integrity of a remote file or reinstalling a remote file. The Appellant argues that Winburn's protected data file is not a physically remote file.

The examiner respectfully disagrees. Winburn discloses that the protected data file is called the authorized protected data file when the protected data file is the original protected data file or the original protected data file modified or accessed by an authorized modification or user. In the description of the invention, the protected data file is called the current protected data file when it is monitored on a time or event driven or other basis as would be now or later known by those skilled in the art, for a representative comparison with the authorized protected data file to determine if the current protected data file has been changed from the authorized protected data file or when a change has occurred and it is not known if a change or access of a protected data file has been an authorized change or access by an authorized user [0025].

E. The Appellant argues that Winburn does not disclose “communicating the request by the authentication module to the install module in a login page that instantiated the file at the remote location," as recited in claim 1 and similarly recited in claim 10.

The examiner respectfully disagrees. Winburn discloses that upon the indication (59), of a difference between the identifier stored in the recovery data group 35 in active memory 14 for the authorized protected data file 31, with the test identifier produced for the current protected file, the processor 13, 16, accesses and reads (63) the recovery indica from the recovery address group 35 and representing the camouflaged authentic backup file 35 and uses that indica to locate and retrieve (65) the authentic backup file 33, file, decrypt it using the stored decryption key and decompress it, deleting the compressed file and using the authentic data backup file to reconstructed authorized protected data file 31, (69) and to write it to the current protected data file 31, (71) to restore the current protected data file with the reconstructed copy, of the authorized protected data file 31 as it was in its last authorized data state and stored as the authentic backup file 33 [0031].

**(11) Related Proceeding(s) Appendix**

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Aravind K Moorthy/

Examiner, Art Unit 2431

Conferees:

William Korzuch

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431

Christopher Revak

/Christopher A. Revak/

Primary Examiner, Art Unit 2431